Fifth NASA Langley Formal Methods Workshop

13-15 June 2000

Radisson Fort Magruder Hotel & Conference Center

Williamsburg, Virginia

http://shemesh.larc.nasa.gov/fm/Lfm2000/

Final Program

Unless otherwise indicated, all sessions are in Newmarket Hall.

Sponsored by the Formal Methods Team, Assessment Technology Branch,
Airborne Systems, NASA Langley Research Center

Tuesday 13 June 2000

8:30	-	8:45	Welcome and Opening Remarks Michael Holloway, Lfm2000 Chairman Luat Nguyen, Deputy Director Airborne Systems Competency
8:45	-	9:30	Using Risk Assessments to Guide the Formal Development of Safety-Critical Systems Chris Johnson, University of Glasgow (invited speaker)
9:30	-	10:00	*break*
			Modeling techniques, chaired by Kelly Hayhurst
10:00	-	10:25	On Tableau Constructions for Timing Diagrams Kathi Fisler, Rice University
10:30	-	10:55	Abstraction Relationships for Real-Time Specifications Monica Brockmeyer, Wayne State University
11:00	-	11:25	Algebra of Behavior Tables Steven D. Johnson and Alex Tsow, Indiana University
11:25	-	1:30	*lunch on your own*
			Hybrid systems & mathematical modeling, chaired by Victor Carreño
1:30	-	1:55	Modeling and Validating Hybrid Systems using VDM and Mathematica Bernhard K. Aichernig and Reinhold Kainhofer, Technical University Graz, Austria
2:00	-	2:25	Modeling the Fault Tolerant Capability of a Flight Control System: An Exercise in SCR Specification Chris Alexander, Azimuth Inc.; Vittorio Cortellessa, West Virginia University (WVU); Diego Del Gobbo, WVU; Ali Mili, WVU; Marcello Napolitano, WVU
2:30	-	2:55	Towards Formal Methods for Mathematical Modelling Ursula Martin, SRI International and University of St. Andrews
2:55	-	3:30	*break*
			Real time analysis, chaired by Gerald Lüttgen
3:30	-	3:55	Applying Model Checking & Abstraction to Verify Time Partitioning in the DEOS Scheduler Kernel John Penix and Willem Visser, NASA Ames Research Center; Eric Engstrom, Aaron Larson, and Nicholas Weininger, Honeywell Technology Center
4:00	-	4:25	Timing Analysis by Model Checking Dimitri Naydich and David Guaspari, Odyssey Research Associates
4:30	-	4:55	Modeling and Verification of Real-Time Software Using Extended Linear Hybrid Automata Steve Vestal, Honeywell Technology Center
6:30	-	8:30	***Reception in a Civil War Redoubt***

Wednesday 14 June 2000

8:30	-	8:45	Opening Remarks (if necessary)
			Recent NASA Langley work, chaired by Ricky Butler
8:45	-	9:10	Analysis of the SPIDER Fault-Tolerance Protocols Paul Miner, NASA Langley Research Center
9:15	-	9:40	Aircraft Trajectory Modeling and Analysis: A Challenge to Formal Methods Victor Carreño, NASA Langley Research Center; César Muñoz, ICASE
9:40	-	10:15	*break*
			Hardware specification and verification, chaired by Paul Miner
10:15	-	10:40	Orpheus: A Self-Checking Translation Tool Arrangement for Flight Critical Hardware David Greve and Matthew Wilding, Rockwell Collins; Mark Bickford and David Guaspari, Odyssey Research Associates
10:45	-	11:10	FormalCORE™ PCI/32 - A Formally Verified VHDL Synthesizable PCI Core Bhaskar Bose, M. Esen Tuna, and Ingo Cyliax, Derivation Systems, Inc.
11:15	-	11:40	Structuring Formal Control Systems Specifications for Reuse Jeffrey M. Thompson, Mats P.E. Heimdahl, and Debra M. Erickson, University of Minnesota
11:40	-	1:00	*lunch on your own*
			Tutorial session 1 (Choose one of the four to attend)
1:00	-	3:00	Model Checking Foundations Edmund Clarke, Carnegie Mellon University — *Davis Amphitheater A*
1:00	-	3:00	Abstract State Machines and their Industrial Employment: A Survey Egon Boerger, University of Pisa (visiting Microsoft Research) — *Lee's Redoubt*
1:00	-	3:00	Formal Hardware Synthesis Using DRS Bhaskar Bose and M. Esen Tuna, Derivation Systems, Inc. — *Grant's Redoubt*
1:00	-	3:00	Automated First-Order Theorem Proving in Software Engineering Johann Schumann, Caelum Research — *Davis Amphitheater B*
3:00	-	3:30	*break*
			Tutorial session 2 (Choose one of the four to attend)
3:30	-	5:30	Software Model Checking Tools and Trends at NASA Klaus Havelund, Recom Technologies; Charles Pecheur and Willem Visser, RIACS; Reid Simmons, Carnegie Mellon University — *Davis Amphitheater A*
3:30	-	5:30	Model Checking & Limiting State Explosion E. Allen Emerson, University of Texas at Austin — *Davis Amphitheater B*
3:30	-	5:30	The Algebraic Specification Language CASL Markus Roggenbach, University of Bremen — *Grant's Redoubt*
3:30	-	5:30	Developing Correct Software with AutoFocus & Quest Oscar Slotosch, Technische Universität München — *Lee's Redoubt*

Thursday 15 June 2000

8:30	-	8:45	Opening Remarks (if necessary)
8:45	-	9:30	Formal Methods Adoption: What's Working? What's Not! Dan Craigen, ORA Canada (invited speaker)
9:30	-	10:00	*break*
			Lightweight methods, chaired by César Muñoz
10:00	-	10:25	Automated V&V for High Integrity Systems, A Targeted Formal Methods Approach Simon Burton, John Clark, Andy Galloway, and John McDermid, University of York
10:30	-	10:55	Integrating Z and Cleanroom Allan M. Stavely, New Mexico Tech
11:00	-	11:25	Applying Use Case Maps and Formal Methods to the Development of Wireless Mobile ATM Networks Rossana M. C. Andrade, University of Ottawa
11:25	-	1:30	*lunch on your own*
			Middleweight methods, chaired by Ben Di Vito
1:30	-	1:55	Formal Analysis of the Remote Agent Before and After Flight Klaus Havelund, Recom Technologies; Mike Lowry, NASA Ames Research Center (ARC); SeungJoon Park, RIACS; Charles Pecheur, RIACS; John Penix, ARC; Willem Visser, RIACS; Jon L. White, Caelum
2:00	-	2:25	Taking the hol out of HOL Nancy A. Day, Oregon Graduate Institute; Michael R. Donat and Jeffrey J. Joyce, Intrepid Critical Software Inc.
2:30	-	2:55	An Overview of SAL Saddek Bensalem, Vijay Ganesh, Yassine Lakhnech, César Muñoz, Sam Owre, Harald Rueß, John Rushby, Vlad Rusu, Hassen Saïdi, N. Shankar, Eli Singerman, Ashish Tiwari, SRI International
2:55	-	3:30	*break*
			A great debate, moderated by Michael Holloway
3:30	-	5:00	Considering the motion: "*This house believes that formal methods are the only intellectually defensible means for addressing the potential of hazardous design faults in digital systems*" For the motion: John Knight, University of Virginia; George Romanski, Verocel Against the motion: Egon Boerger, University of Pisa (visiting Microsoft Research); Mats P.E. Heimdahl, University of Minnesota